E. MARTIN ESTRADA
United States Attorney
CAMERON L. SCHROEDER
Assistant United States Attorney
Chief, National Security Division
KHALDOUN SHOBAKI
Assistant United States Attorney,
Chief, Cyber & Intellectual Property Crimes Section
JONATHAN GALATZAN
Assistant United States Attorney
Chief, Asset Forfeiture and Recovery Section
MAXWELL COLL (Cal. Bar No. 312651)
Assistant United States Attorney
National Cryptocurrency Enforcement Team
Computer Crime & Intellectual Property Section
312 North Spring Street
Los Angeles, California 90012
Telephone: (213) 894-1785
Facsimile: (213) 894-0142
E-mail: Maxwell.Coll@usdoj.gov

JESSICA PECK
Trial Attorney, U.S. Department of Justice
Computer Crime & Intellectual Property Section
1301 New York Ave., N.W., Suite 600
Washington, D.C. 20005

Attorneys for Plaintiff
UNITED STATES OF AMERICA

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Plaintiff, v. $1,168,679 IN FUNDS ASSOCIATED WITH TWO STABLECOIN ADDRESSES ON THE ETHEREUM NETWORK, Defendant.	No. 2:24-cv-4640 **VERIFIED COMPLAINT FOR FORFEITURE** 18 U.S.C. § 981(a)(1)(A) and (C)

Plaintiff United States of America brings this claim against defendant $1,168,679 in Funds Associated with Two Stablecoin Addresses on the Ethereum Network (the "defendant funds"), and alleges as follows:[1]

JURISDICTION AND VENUE

1. Plaintiff United States of America brings this in rem forfeiture action pursuant to 18 U.S.C. § 981(a)(1)(A) and (C).

2. This Court has jurisdiction over civil actions commenced by the United States of America under 28 U.S.C. § 1345 and over forfeiture actions under 28 U.S.C. § 1355(a).

3. Venue lies in this District pursuant to 28 U.S.C. § 1355(b)(1) because acts or omissions giving rise to the forfeiture occurred in this District. Venue also lies in this District pursuant to 28 U.S.C. § 1395(c) because the defendant funds are presently located in this District in a government-controlled account.

PERSONS AND ENTITIES

4. The plaintiff is the United States of America.

5. The defendant funds are the U.S. dollar equivalent of USDC, which is a "stablecoin" type of virtual currency pegged to the U.S. dollar as discussed below, associated with the following virtual currency addresses on the Ethereum network:

a. 1,108,586 USDC associated with a virtual currency address ending in "16ce8" (the "Virtual Currency Address 1"); and

b. 60,093 USDC associated with a virtual currency address ending in "eBDca" (the "Virtual Currency Address 2," and together with Virtual Currency Address 1, the "Virtual Currency Addresses").

[1] All dates set forth in this Complaint are on or about the dates indicated, and all amounts or sums are approximate.

6. On February 2, 2023, the Department of Justice caused the freeze of the USDC in Virtual Currency Address 1 and Virtual Currency Address 2, and on August 18, 2023, a seizure warrant was obtained which resulted in the transfer of the defendant funds to the Federal Bureau of Investigation ("FBI") on September 20, 2023.

7. The defendant funds are held in the custody of the United States Marshals Service, where the defendant funds shall remain subject to this Court's jurisdiction pending the resolution of this action.

8. The interests of the victim Harmony, a U.S.-based open-source blockchain network for decentralized virtual currency applications, and other victims identified further herein may be adversely affected by these proceedings.

BASIS FOR FORFEITURE

9. The defendant funds are subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A) and (C) because they constitute traceable proceeds of and were involved in money laundering offenses pertaining to the theft of virtual currency by the North Korean military hacking group known as, among other names, the Lazarus Group and Advanced Persistent Threat 38 ("APT38").

I. Definitions and Background Related to Virtual Currency

10. **Virtual Currency**: Virtual currencies are digital tokens of value circulated over the internet as substitutes for traditional fiat currency. Virtual currencies are not issued by any government or bank like traditional fiat currencies, such as the U.S. dollar, but rather are generated and controlled through computer software. Bitcoin (or "BTC") and ether ("ETH") are currently the most well-known virtual currencies in use.

11. **Stablecoins**: Stablecoins, while also a type of virtual currency, are unlike BTC and ETH because stablecoins are pegged to a commodity's price, such as gold, or to a fiat currency, such as the U.S. dollar. Stablecoins achieve their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives. USDC is a popular stablecoin. It is pegged to the U.S. dollar.

12. **Virtual Currency Address**: Virtual currency addresses are the particular virtual locations to which such currencies are sent and received. A virtual currency address is analogous to a bank account number and is represented as a string of letters and numbers.

13. **Private Key**: Each virtual currency address is controlled through the use of a unique corresponding private key, a cryptographic equivalent of a password, which is needed to access the address. Only the holder of an address's private key can authorize a transfer of virtual currency from that address to another address.

14. **Virtual Currency Wallet**: There are various types of virtual currency wallets, including software wallets, hardware wallets, and paper wallets. The virtual currency wallets at issue for the purposes of this complaint are software wallets (i.e., a software application that interfaces with the virtual currency's specific blockchain and generates and stores a user's addresses and private keys). A virtual currency wallet allows users to store, send, and receive virtual currencies. A virtual currency wallet can hold many virtual currency addresses at the same time.

15. Wallets that are hosted by third parties are referred to as "hosted wallets" because the third party retains a customer's funds until the customer is ready to transact with those funds.

Conversely, wallets that allow users to exercise total, independent control over their funds are often called "unhosted" wallets.

16. **Blockchain**: Many virtual currencies publicly record all of their transactions on what is known as a blockchain. The blockchain is essentially a distributed public ledger, run by the decentralized network of computers, containing an immutable and historical record of every transaction utilizing that blockchain's technology. The blockchain can be updated multiple times per hour and records every virtual currency address that has ever received that virtual currency and maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies.

17. **Blockchain Explorer**: These explorers are online tools that operate as a blockchain search engine allowing users the ability to search for and review transactional data for any addresses on a particular blockchain. A blockchain explorer is software that uses APIs[2] and blockchain nodes to draw data from a blockchain and uses a database to arrange and present the data to a user in a searchable format.

18. **Decentralized Finance (DeFi)**: Decentralized Finance, or DeFi, is an umbrella term for financial services on public blockchains, primarily the Ethereum network. The Ethereum network's native virtual currency is ETH. Ethereum was the first blockchain that offered various decentralized services within its network. To make these services possible, the Ethereum network allows other

[2] APIs stands for application programming interfaces, which are a set of definitions and protocols for building and integrating application software.

tokens besides ETH to run within the network. These tokens are known as ERC-20 tokens.

19. DeFi is a term used to describe a financial system that operates without the need for traditional, centralized intermediaries. Instead, DeFi platforms offer an alternative financial system that is open for anyone to use, and that allows centralized intermediaries to be replaced by decentralized applications (or dApps). With DeFi, one can do most of the things that banks support--earn interest, borrow, lend, buy insurance, trade derivatives, trade assets, etc.--but it is faster than using traditional banks and does not require paperwork or a third party. DeFi is global, peer-to-peer (i.e., directly between two people rather than routed through a centralized system), pseudonymous, and open to the public.

20. **Virtual Currency Bridge**: A blockchain bridge, otherwise known as a cross-chain bridge, connects blockchains and allows users to send virtual currency from one blockchain to the other.

21. **Virtual Currency Exchanges (VCEs)**: VCEs are trading and/or storage platforms for virtual currencies, such as BTC and ETH. There are generally two types of VCEs: centralized exchanges and decentralized exchanges, which are also known as "DEXs." Many VCEs (both centralized and DEXs) also store their customers' virtual currency in virtual currency wallets. As previously stated, these wallets can hold multiple virtual currency addresses associated with a user on a VCE's network. Because VCEs act as money services businesses, they are legally required to conduct due diligence of their customers and to have anti-money laundering programs in place

(to the extent they operate and service customers in the United States).

22. **Virtual Currency Mixers**: Virtual-currency mixers (also known as tumblers or mixing services) are software services that allow users, for a fee, to send virtual currency to designated recipients in a manner designed to conceal and obfuscate the source of the virtual currency.

23. **Blockchain Analysis**: As previously stated, while the identity of a virtual currency address owner is generally anonymous, law enforcement can identify the owner of a particular virtual currency address by analyzing the blockchain (e.g., the BTC blockchain). The analysis can also reveal additional addresses controlled by the same individual or entity.

II. North Korean Cyberattacks and Virtual Currency Heists

24. The Lazarus Group is responsible for numerous high-profile international virtual currency heists. For example, in August 2021, North Korean hackers stole approximately $90 million in virtual currency from Japan-based virtual currency exchange Liquid. In March 2022, North Korean hackers stole over $600 million in virtual currency from Sky Mavis, the company behind Axie Infinity, a popular blockchain-based play-to-earn video game. In June 2023, North Korean hackers stole approximately $60 million in virtual currency from Alphapo, a centralized virtual currency payment provider, and approximately $37 million in virtual currency from CoinsPaid, another virtual currency payment platform.

25. As is relevant for the purposes of this complaint, the North Korean cyber hackers initially conducted a cyberattack against Sony Pictures Entertainment in the Central District of California in

November and December 2014. In February 2021, the government unsealed an indictment charging three members of the North Korean military who were part of this ongoing conspiracy in Central District of California Case No. 2:20-CR-614-MCS. The North Korean hackers who stole virtual currency from Liquid, Sky Mavis, and Harmony are part of the same ongoing conspiracy and have regularly used U.S.-based computer infrastructure, including computers located in the Central District of California, to facilitate intrusions that are part of these virtual currency heists.

III. Horizon Bridge Hack and Laundering of the Defendant Funds

26. Harmony is a U.S.-based open-source blockchain network for decentralized virtual currency applications. Harmony developed Horizon, a virtual currency bridge, which connects blockchains and allows users to send virtual currency from one blockchain to another.

27. On June 23, 2022, North Korean hackers stole approximately $105 million worth of virtual currency from Harmony's virtual currency bridge, Horizon. The North Korea hackers used a malware campaign dubbed "TraderTraitor" by the United States government. As part of the campaign, the hackers promoted malicious applications that resembled virtual currency trading or price-prediction tools, but in reality, those tools were malware used to infiltrate the Horizon bridge infrastructure.

A. Laundering of Virtual Currency, Which Included the Defendant Funds, Through Tornado Cash

28. The North Korean hackers infiltrated the Horizon bridge service and funneled batches of ETH through a virtual currency mixer

known as Tornado Cash.[3] Tornado Cash operated on the Ethereum blockchain and indiscriminately facilitated anonymous transactions by obfuscating their origin, destination, and counterparties, with no attempt to determine their origin.

29. A hacker-controlled Ethereum address ending in "DeD00" served as an initial consolidation point for stolen funds following the Horizon Bridge theft, and received approximately 85,870 stolen ETH[4] that originated from the Horizon bridge. This address then sent funds on June 27, 28, 29, and 30, and July 1, 2022, to several Ethereum addresses, which subsequently funneled a total of 85,700 ETH into the Tornado Cash mixer. On each date, funds were further broken down into smaller batches before being sent through Tornado Cash. Each batch of ETH contained a value between $6.4 million and $8.2 million in virtual currency in increments of 100 ETH. (These valuations in U.S. dollars have been calculated based on the price of ETH at the time of the transactions.) In total, hackers sent 14 batches of funds through Tornado Cash to obfuscate the tracing of these transactions.

B. Use of Dormant Addresses and Railgun Privacy Protocol To Further Launder The Defendant Funds

30. North Korean hackers next withdrew the funds from Tornado Cash and transferred the virtual currency to various Ethereum addresses, where it sat dormant for months. From July 3, 2022, until

---

[3] On August 8, 2022, the U.S. Treasury Department's Office of Foreign Assets Control ("OFAC") sanctioned Tornado Cash because it had been used to launder more than $7 billion worth of virtual currency, including over $455 million stolen by the Lazarus Group.

[4] On June 27, 2022, 1 ETH traded at $1,191.27 and on July 1, 2022, 1 ETH traded at $1,057.57.

January 11, 2023, the ETH sat dormant, largely unspent in approximately 149 virtual currency addresses.

31. On January 11, 2023, hackers initiated two transactions of ETH from the previously dormant virtual currency addresses through Railgun, a so-called privacy protocol built on the Ethereum blockchain. After these initial test transactions, on or about January 13 and 14, 2023, hackers transferred a wave of seven batches of post-Tornado Cash ETH from 70 different Ethereum addresses into the Railgun protocol. The total amount of ETH transferred into the Railgun protocol was 41,792.47 ETH, which at the time held a value of over $60 million.

C. Conversion of Defendant Funds from ETH to BTC

32. North Korean hackers then transferred ETH to three virtual currency exchanges to convert the stolen ETH into BTC. On January 13 and 14, 2023, North Korea-affiliated BTC addresses received and sent 1,656.13 BTC, worth approximately $33.8 million. Funds were subsequently removed from these BTC addresses between on or about January 15 and January 20, 2023. Approximately 559.9997 BTC was reconsolidated at a single virtual currency address.

D. Conversion of Defendant Funds from BTC to Stablecoin USDC

33. After reconsolidating (this time in the form of BTC), the hackers converted the BTC to USDC. On February 1 and 2, 2023, a BTC address ending in "4slaf" sent approximately 50.10 BTC (valued at approximately $1,184,217.00 at the time of the transaction) to a virtual currency bridge in 12 separate transactions. The blockchain bridge was used to convert the BTC (proceeds of the Horizon bridge cyberattack) into USDC.

34. Hackers bridged the BTC funds to USDC, transferring the proceeds to the Virtual Currency Addresses.

E. Seizure and Transfer of Defendant Funds

35. On February 2, 2023, the Department of Justice caused the freeze of the USDC associated with the Virtual Currency Addresses. The Department of Justice subsequently obtained a federal seizure warrant for the defendant funds and caused the transfer of the defendant funds to the United States.

36. The defendant funds are currently in the possession of the United States government.

FIRST CLAIM FOR RELIEF

(18 U.S.C. § 981(a)(1)(A))

37. Paragraphs 1 through 36 are incorporated by reference as if fully set forth herein.

38. The defendant funds are property involved in, or traceable to property involved in, a transaction in violation of 18 U.S.C. §§ 1956(a)(1)(A)(i), 1956(a)(1)(B)(i), 1956(a)(2)(A), 1956(a)(2)(B)(i), 1956(h), and 1957.

39. For purposes of 18 U.S.C. §§ 1956 and 1957, "specified unlawful activity" includes, among other things, "an offense under . . . section 1030 (relating to computer fraud and abuse)." 18 U.S.C. § 1956(c)(7)(D).

40. As set forth above:

a. the defendant funds are property involved in, or are traceable to property involved in, a financial transaction or attempted financial transaction involving the proceeds of an offense of accessing a computer to defraud and obtain value, which transaction or attempted transaction was conducted with the knowledge that the property involved in the transaction represented the proceeds of some form of unlawful activity and with the intent to promote the carrying on of specified unlawful activity in violation of 18 U.S.C. § 1956(a)(1)(A)(i);

b. the defendant funds are property involved in, or are traceable to property involved in, a financial transaction or attempted financial transaction involving the proceeds of an offense of accessing a computer to defraud and obtain value, which transaction or attempted transaction was conducted with the knowledge that the property involved in the transaction or attempted

transaction represented the proceeds of some form of unlawful activity and that the transaction or attempted transaction was designed in whole or in part to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity in violation of 18 U.S.C. § 1956(a)(1)(B)(i);

c. the defendant funds are property involved in, or are traceable to property involved in, the transportation, transmission, or transfer, or the attempted transportation, transmission, or transfer, of a monetary instrument or funds from a place in the United States to or through a place outside the United States with the intent to promote the carrying on of an offense of accessing a computer to defraud and obtain value in violation of 18 U.S.C. § 1956(a)(2)(A);

d. the defendant funds are property involved in, or are traceable to property involved in, the transportation, transmission, or transfer, or the attempted transportation, transmission, or transfer, of a monetary instrument or funds to a place outside the United States from or through a place inside the United States, with the knowledge that the monetary instruments or funds represented the proceeds of some form of unlawful activity and with the knowledge that the transportation, transmission, or transfer, or attempted transportation, transmission, or transfer, was designed in whole or in part to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of an offense of accessing a computer to defraud and obtain value in violation of 18 U.S.C. § 1956(a)(2)(B)(i);

e. the defendant funds are property involved in, or are traceable to property involved in, a monetary transaction or attempted monetary transaction, affecting interstate or foreign commerce, in criminally derived property of a value greater than $10,000 derived from an offense of accessing a computer to defraud and obtain value, which transaction or attempted transaction was conducted with the knowledge that the property involved was criminally derived in violation of 18 U.S.C. § 1957; and

f. the defendant funds are property involved in, or traceable to property involved in, a conspiracy in violation of 18 U.S.C. § 1956(h). Specifically, the defendant funds are property involved in, or traceable to property involved in, a conspiracy to commit the violations of 18 U.S.C. §§ 1956(a)(1)(A)(i), 1956(B)(i), 1956(a)(2)(A), 1956(a)(2)(B)(i), and 1957 set forth in subparagraphs 40(a) through (e) above.

41. For each of the above reasons, the defendant funds are subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A).

SECOND CLAIM FOR RELIEF

(18 U.S.C. § 981(a)(1)(C))

42. Paragraphs 1 through 35 are incorporated by reference as if fully set forth herein.

43. The defendant funds are property that constitutes, or is derived from, proceeds traceable to an offense of accessing a computer to defraud and obtain value, which is a violation of 18 U.S.C. § 1030(a)(4), or a conspiracy to commit such an offense.

44. The defendant funds are therefore subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff the United States of America prays:

(a) that due process issue to enforce the forfeiture of the defendant funds;

(b) that due notice be given to all interested parties to appear and show cause why forfeiture should not be decreed;

(c) that this Court decree forfeiture of the defendant funds to the United States of America for disposition according to law; and

(d) for such other and further relief as this Court may deem just and proper, together with the costs and disbursements of this action.

Dated: June 4, 2024

E. MARTIN ESTRADA
United States Attorney

CAMERON L. SCHROEDER
Assistant United States Attorney
Chief, National Security Division

KHALDOUN SHOBAKI
Assistant United States Attorney,
Chief, Cyber & Intellectual Property Crimes Section

/s/ Maxwell Coll
MAXWELL COLL
Assistant United States Attorney
National Cryptocurrency Enforcement Team, Computer Crime & Intellectual Property Section

JESSICA PECK
Trial Attorney,
U.S. Department of Justice
Computer Crime & Intellectual Property Section
1301 New York Ave., N.W., Suite 600
Washington, D.C. 20005

Attorneys for Plaintiff
UNITED STATES OF AMERICA

VERIFICATION

I, Justin Vallese, hereby declare that:

1. I am a Special Agent with the Federal Bureau of Investigation.

2. I have read the above Complaint for Forfeiture and know the contents thereof.

3. The information contained in the Complaint is either known to me personally, was furnished to be my official government sources, or was obtained pursuant to legal process. I am informed and believe that the allegations set out in the Complaint are true.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on June 3, 2024, at Los Angeles, California.

Justin Vallese